What Is Claimed Is:

1. A method for registering a first device with a second device, comprising the steps of:

generating a first secret known to the first device and a second secret known to the second device using communications between the first device and the second device over a first communication channel, said first and second secrets ostensibly being the same;

from the first device, producing first information derived from the first secret;

from the second device, producing second information derived from the second secret;

using a communication channel other than the first communication channel, comparing the first information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same; and

enabling the first and second device to use the first and second secrets upon the third party being assured that the first secret and the second secret are the same.

2. The method of claim 1 wherein the first device and the second device generate the first and second secrets using a Diffie-Hellman key exchange.

3. The method of claim 1 wherein:

the first information is derived from a hash of the first secret; and

the second information is derived from a hash of the second secret.

4. The method of claim 1 wherein the first information comprises a credential.

5. A method for registering a first device with a second device, comprising the steps of:

(a) communicating a commitment from the first device to the second device over a first communication channel, said commitment comprising information derived from a security value known to the first device;

(b) communicating from the second device to the first device over the first communication channel, information for use in generating a first secret;

(c) after step (b), communicating the security value from the first device to the second device;

(d) generating the first secret at the first device and a second secret at the second device, said first and second secrets ostensibly being the same;

(e) from the first device, on a communication channel other than the first communication channel, validating first verification information related to the first secret;

(f) from the second device, on a communication channel other than the first communication channel, validating second verification information related to the second secret; and

(g) enabling the first and second devices to use the first and second secrets upon a third party being assured that the first secret and the second secret are the same.

6. The method of claim 5 wherein the commitment is a hash of the security value.

7. The method of claim 5 wherein the first verification information is a hash value derived from the first secret and the security value.

8. The method of claim 7 wherein the first verification information is a hash value derived from a catenation of the first secret with the security value.

9. The method of claim 5 wherein the length of the first verification information is shorter than a length needed to provide a substantially identical level of security in a substantially identical method that does not utilize said commitment.

10. The method of claim 5 wherein the first verification information comprises a credential.

11. A device capable of registering with an other device, comprising:

an interface to a first communication channel;

an interface to a second communication channel;

a registration process that (1) generates a first secret that is ostensibly shared with the other device using the first communication channel, (2) validates on the second communication channel verification information derived from the ostensibly shared secret, and (3) is enabled to use the ostensibly shared secret upon receipt of an indication that a third party is assured that the first secret is shared with the other device.

12. The device of claim 11 wherein the device generates the first secret using a Diffie-Hellman key exchange.

13. The device of claim 11 wherein the verification information is derived from a hash of the first secret.

14. The device of claim 11 wherein the verification information comprises a credential.

15. A device capable of registering with an other device, comprising:

an interface to a first communication channel;

an interface to a second communication channel;

a registration process that (1) receives, on the first communication channel, a commitment derived from a security value; (2) produces, on the first communication channel, information for use in generating a shared secret; (3) after step (2), communicates the security value on the first communication channel; (4) generates a first secret ostensibly shared with the other device, (5) communicates on the second communication channel verification information related to the first secret, and (6) is enabled to use the first secret upon receipt of an indication that a third party is assured that the first secret is shared with the other device.

16. The device of claim 15 wherein the commitment is a hash of the security value.

17. The device of claim 15 wherein the verification information is a hash value derived from the first secret and the security value.

18. The device of claim 17 wherein the verification information is a hash value derived from the catenation of the first secret with the security value.

19. The device of claim 15 wherein the length of the verification information is shorter than a length needed to provide a substantially identical level of security in a substantially identical method that does not utilize said commitment.

20. The method of claim 15 wherein the verification information is a credential.

21. A server capable of registering a device to a network, comprising:

an interface to a first communication channel;

an interface to a second communication channel; and

a registration process that (1) generates a first secret that is ostensibly shared with the device using the first communication channel; (2) validates on the second communication channel verification information derived from the first secret, and (3) enables the network to use the first secret upon receipt of an indication that a third party is assured that the ostensibly shared secret is shared with the device.

22. The server of claim 21 wherein the server generates the first secret using a Diffie-Hellman key exchange.

23. The server of claim 21 wherein the verification information is derived from a hash of the first secret.

24. The server of claim 21 wherein the verification information comprises a credential.

25. A server capable of registering a device to a network, comprising:

an interface to a first communication channel;

an interface to a second communication channel; and

a registration process that (1) communicates over the first communication channel a commitment comprising information derived from a security value; (2) communicates over the first communication channel information for use in generating a shared secret; (3) after step (2), communicates the security value over the first communication channel; (4) generates a first secret ostensibly shared with the device; (5) communicates over the second communication channel verification information related to the secret; and (6) enables the network to use the first secret upon receipt of an indication that a third party is assured that the first secret is shared with the device.

26. The server of claim 25 wherein the commitment is hash of the security value.

27. The server of claim 25 wherein the verification information is a hash value derived from the secret and the security value.

28. The server of claim 27 wherein the verification information is a hash value derived from the catenation of the first secret with the security value.

29. The server of claim 25 wherein the length of the verification information is shorter than a length needed to provide a substantially identical level of security in a substantially identical method that does not utilize said commitment.

30. The method of claim 25, wherein the verification information comprises a credential.